WCIT Proposals to Watch (based on matrix TD62 rev1)[1]

There have been a number of substantive topics proposed for inclusion in the ITRs.[2] These range from more technical issues such as critical Internet resources, routing regulation, numbering misuse, and quality of service, to policy and content issues such as cybersecurity, cybercrime, data protection, spam, and child online protection. Current government proposals vary in level of detail, so it can be difficult to assess the actual impact on freedom of expression, privacy, and other human rights for some of the proposals at this time – in part, the impact will depend on how the proposal is implemented in national law and how broadly definitions are interpreted. Some current proposals continue to be merely placeholders, to be expanded later, and governments will continue to add or amend proposals up to and during the WCIT in December.

However, there are some categories of proposals that are already clearly going to be the focus of a lot of attention during the WCIT process, and which raise concerns for privacy, freedom of expression, and the technical functioning of the global Internet. Here is a compilation of some of the more worrying proposals, with references to page numbers in TD62 rev1. We also provide a list of acronyms at the end of this document.

A. Cybersecurity, cybercrime, and privacy

1. Cybersecurity, cybercrime, and privacy

- There is a vocal contingent of Member States arguing that the ITRs should address cybersecurity, network security, and cybercrime. Current proposal language is very broad and could go beyond telecom and reach into areas of national security and law enforcement
- Proposals are coming in the form of wholly new provisions in the treaty that did not exist before. For the most part, the language of the proposals is fairly high-level and is framed in terms of cooperation and harmonization of national approaches. There may be additional proposals relating to cybersecurity generated at the regional and national level between now and the end of June.
- The concerns about privacy here will vary depending on the specifics of the proposal (and there is a range). However, even the mildest language that encourages greater cooperation may be worrisome as it represents incremental mission creep by an institution not well positioned to carefully weigh equally important interests like security and privacy, or analyze specific implementations of treaty obligations with their consistency with human rights standards. Other proposals encourage greater harmonization of national law on issues like data retention, which may encourage broader adoption of laws that do not adequately safeguard privacy.
- Many of the proposals conflate very different aspects of “security” that, in current ongoing policy discussions, require very different solutions. For example, there is no distinction made in many proposals between state-sponsored cyberattacks used for military purposes (which raises law of war issues), and issues like malware, phishing, spam or cybercrime (broadly referenced). While governments have legitimate concerns in all of these areas, the policy response to each will be – and should be – very different. Each policy issue requires careful balancing and consideration of impact on privacy and

[1] http://files.wcitleaks.org/public/T09-CWG.WCIT12-120620-TD-PLEN-0062!R1!MSW-E.pdf. Note that this analysis will be constantly updated and a new revision of the compiled proposals has already been released since this memo was drafted.
[2] Text of the ITRs is available here: http://www.itu.int/oth/T3F01000001

expression.

- In favor:
  - The proposals come from a variety of sources: China, the Arab States regional group (pg. 66-67, Art. 3.3), Russia (pg. 142-143, new Art. 8; pg. 148-149 new Art. 10), the Regional Commonwealth in the field of Communications (RCC) (pg. 141-142, new Art. 8), Egypt (pg. 67, Art. 3.3; pg. 149-150 new Art.), Algeria (pg. 137 Art. 8.2), and Côte d'Ivoire (pg. 88, Art. 4.3a). CEPT, the European regional group, and the Asia-Pacific Telecommunity (pg. 140, Art. 8.5) have also developed a proposal to encourage Member State cooperation (pg. 154 new Art.).
  - China ("Member States have the responsibility and right to protect the network security of the information and communication infrastructure within their state. . . . Member State have the responsibility to require and supervise that enterprises operating in their territory protect the security of user information." TD 62 pg. 138-139, Art. 8.5)
  - In a somewhat more detailed proposal, the Regional Group for Africa proposed a new article stating that Member States "should cooperate regarding telecommunications security matters (including cybersecurity), in particular to develop technical standards and acceptable legal norms" which would include issues of jurisdiction and sovereign responsibility. (pg. 153-154, new Art.) Member States "shall cooperate to harmonize national laws, jurisdictions, and practices" for prosecution of cybercrime, data retention, preservation, and protection; "and approaches to network defense and response to cyberattacks."
  - Recently, the Arab States have proposed an entirely new article on "confidence and security of telecommunications/ICTs", which includes a definition that "Issues related to security include physical and operational security; cybersecurity, cybercrime, and cyber attacks; denial of service attacks; other online crime; controlling and countering unsolicited electronic communication (e.g. spam); and protection of information and personal data (e.g. phishing)." This new article would instruct Member States to "cooperate to investigate, prosecute, correct, and repair security breaches and incidents in a timely manner," to "ensure that operating agencies and other concerned entities provide and maintain, to the greatest extent practicable, confidence and security of telecommunications/ICTs" and "cooperate with their counterparts in other Member States in ensuring confidence and security of telecommunications/ICTs." (C 103 Arab States)
  - At the African Telecommunication Union regional meeting in May, the RCC and Russia proposals on cybersecurity did not get any traction; Tanzania and Uganda specifically indicated the intent to focus on the general principle of cooperation between member states
  - From CEPT, the European regional group, in May: "Member states should encourage operating agencies to take measures to further the security, safety, continuity, sustainability and robustness of their networks used for international telecommunications services. Member States are encouraged to cooperate in that sense." (pg. 154, new Art.)
  - CITEL has not yet agreed to an Inter-American Proposal about cybersecurity; there is likely some disagreement within the region about how to proceed
- Against:
  - USA, Australia, Canada

2. National regulation of IP routing to address fraud/security; greater identification

- A number of proposals speak to the need to address fraud and security in telecommunications by regulating telecommunications traffic (see generally Art. 3). If these proposals are limited to the traditional telephone context, then their impact might also be limited. However, if these proposals are extended to Internet technologies (IP networks), each of these issues could raise technical challenges for Internet-based communications, as well as concerns about privacy, anonymity, and access to information online.

- These proposals would allow member states to determine how traffic (communications, information) is routed into their country and impose regulations on routing to prevent security and fraud. Depending on implementation, this could increase governments' ability to identify communications between users and what information users might be accessing online (through IP addresses).
- At heart, if these proposals are applied to internet traffic, it reveals lack of understanding of how Internet traffic is currently routed and could undermine the decentralized nature of the network. Such proposals could potentially lead to additional chokepoints on Internet traffic that could become points of control on the flow of information.
- <u>In favor</u>:
  - Arab States (C 67) ("A Member State shall have the right to know through where its traffic has been routed, and should have the right to impose any routing regulations in this regard, for purposes of security and concerning fraud." Art. 3.3, pg. 66-67)
  - Egypt ("A Member State shall have the right to know through where its traffic has been routed, for purposes of security and concerning fraud." Art. 3.3, pg. 67)
  - Mexico (C 124) ("Operating agencies shall determine by mutual agreement which international routes intend to use and shall duly inform Administrations of State Members involved in said route. Subject to agreement and provided that there is no direct route existing between the operating agencies concerned, the origin operating company, having been previously authorized by involved Administrations, has the choice to determine the routing of its outgoing telecommunication traffic, taking into account the interests of the relevant transit and destination operating agencies.")
- <u>Against</u>: Sweden, UK, USA
  - At African Telecommunication Union regional meeting in May, Member States specifically rejected notion that Member States shall impose routing regulations. But there was a general sense from delegates is that Member States should have a right to know routing.

3. Fraud, misuse, and greater identification

- A number of proposals speak to the need to address fraud and naming, numbering, and addressing misuses in telecommunications, which can include issues of charging arrangements between telecommunications services, controlling use of VoIP, and requiring states or service providers to provide "calling party identification information." (Art. 2.16 (new definition of "fraud", pg. 50-52)). If these proposals are limited to the traditional telephone context, then their impact may be more limited. However, if these proposals are extended to Internet technologies, each of these issues could raise technical challenges for Internet-based communications, as well as privacy concerns for users – especially when combined with proposals to regulate internet traffic routing (A.2. above).
  - "Member States shall ensure that operating agencies duly identify the subscriber when providing international telecommunication services, and shall ensure the appropriate processing, transmission and protection of identification information in international telecommunication networks." Russia (C 95, New Art. 8.2, pg.

142-43)

- **Calling party identification** – There are several variations of this proposal, but in brief, states would require recording and provision of “calling party number” (identifier for where a telephone call is coming from). If limited to telephony context, then impact would be limited. However, if applied to internet traffic, could have much broader impact on privacy if “calling party identification” is interpreted to mean IP address or some other identifier. (Art. 2.18 pg. 54-57; Art. 3.6 pg. 72-77)
    - Some proposals would allow states to mask information other than calling country code and destination country code for privacy reasons, but such information “shall be made available to duly authorized law enforcement agencies” (Egypt, Cote d’Ivoire, Arab States)
    - <u>In favor</u>: Arab States, Egypt (Art. 4.5 pg. 91; Art. 6.10 pg. 121), Cote d’Ivoire (Art. 3.6 pg. 72), Pacific Islands (Art. 3.6 pg. 73), regional group for Asia-Oceania (Art. 3.6 pg. 72), regional group for Latin America (C 25) (Art. 3.6 pg. 73), RCC, Cuba, majority of African countries, Russian Federation (C 40)(Art. 8.4 pg. 138).
    - <u>Against</u>: USA, Canada, CEPT
- **“Naming, Numbering, Addressing, and Identification resource” misuse** (proposals for new Art. 3.7):
    - There are several proposals along this line. One example: “Member States shall ensure that international naming, numbering, addressing and identification resources are used only by the assignees and only for the purposes for which they were assigned; and that unassigned resources are not used.“
    - <u>In favor</u>:
        - Pacific Islands (C 42)(Art. 3.7, pg. 77), Africa (C 43, Study Group 3 of Regional Group for Africa (Art. 3.2, pg. 63; 3.4, pg. 69)), Arab States (C 67)(Art. 3.7, pg. 77), UAE, Iran (C 48)(Art. 3.7 pg. 79), Egypt, Russian Federation (C 40)(Art. 8.3 pg. 138), Algeria (Art. 8.3 pg. 138)
        - Cuba (C 47)(Art. 3.7, pg. 78), UAE(Art. 3.7, pg. 77), Egypt ("The ITRs need to complement the definition of fraud by identifying the scope of the commitments made by members in regard to this issue.")
        - Côte d'Ivoire
    - <u>Against</u>: USA (C45), Australia, Canada,

B. Regulation of Expression and Access to Services

1. Direct regulation of access to infrastructure and services:

- “Member States shall ensure unrestricted public access to international telecommunication services and the unrestricted use of international telecommunications, *except in cases where international telecommunication services are used for the purpose of interfering in the internal affairs or undermining the sovereignty, national security, territorial integrity and public safety of other States, or to divulge information of a sensitive nature*.” Russia (C 95, New Art. 8.2, pg. 142-43)
- This proposal articulates permissible limitations on access and use of telecommunications / telecommunications services in very broad and vague terms, clearly raising risk of misuse and could be used to justify censorship. In addition, because of how the definition of “telecommunication” may change (see immediately below, Section B.2.), the term “telecommunication services” could be interpreted quite broadly to encompass a range of online services such as email, search, or social media.
- This proposal is plainly inconsistent with human rights standards that articulate when governments may permissibly limit the right to freedom of expression under Article 19.

This proposal is also inconsistent with the recommendations made by the UN Special Rapporteur on freedom of opinion and expression in his recent reports on permissible limitations and the Internet, as well as General Comment No. 34 on Article 19 adopted by the Human Rights Committee in 2011.[3]

2. Defining "telecommunication" to include "data processing"

- Proposal to add "data processing" to definition of "telecommunications," which would broaden the ITRs far beyond traditional telecommunications. There is also a proposal to add a definition for "personal data."
- The term "processing" is broad and could potentially be read to sweep in internet services and applications that deal with user data and content, and could sweep in content itself, within the definition of telecommunications. It would represent an enormous expansion of the ITU's mandate, going well beyond basic technical functions and interoperability. The term "processing" also has well-defined (and very broad) meaning under EU data protection laws, which raises questions about how EU member states would implement ITR treaty obligations and how all states might interpret "processing" in the ITR context, given its broader legal use.
- Because this proposal amends a definition that is used throughout the treaty, *all* proposals must be viewed with an understanding that the term "telecommunications" could sweep in online applications and individual expression.
- In favor:
    - Arab States ("Expand the definition [of telecommunication] so it explicitly covers ICTs. Processing takes place after signals are received.")
    - Egypt ("An example of processing is the manipulation or change of calling party number in a transit node.")
    - Mexico ("The addition of 'processing' is justifiable from a technical point of view because processing does take place within networks.")
- Against: Spain, UK, USA, Netherlands, Iran

3. Spam

- Proposals regarding spam seek to encourage greater cooperation and development of technical measures to prevent spam on national networks. But depending on how "spam" is defined, these proposals raise issues of potential restrictions on freedom of expression, access to information, assembly, and association
- In favor:
    - Arab States (C 67), Russian Federation (C 22), Algeria, Egypt (all supporting adding a new definition of spam to ITRs – information transmitted over telecommunications networks bearing advertising nature or having no meaningful message over short period of time to large number of addressees without prior consent of addressees)
        - Depending on how "advertising nature" or "no meaningful message" are defined, could be misused to target activists, human rights campaigners, civil society groups, or political opposition in an election context.
    - RCC proposes a definition of spam that is expansive: "Information transmitted over telecommunications networks simultaneously or during a short period of time to a large number of particular addresses without prior consent of addresses…"
        - Without any limitation that the information must be advertising in nature,

[3] See http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx and http://www2.ohchr.org/english/bodies/hrc/comments.htm

there is even greater risk of misuse.

- CEPT ("Member States are encouraged to adopt national legislation to act against spam, to cooperate to take actions to counter spam, and to exchange information on national findings/actions to counter spam.")

- Against: USA, Australia, Canada, Iran

4. Child protection

- Proposal related to child protection is still quite vague, but the issue generally raises the fear that expression and access to information will be limited in an overbroad way in the name of protection of children
- In favor: Russian Federation (no specific language proposed yet, just noting that it may supply a new definition of "online child protection")

C. Standards and Internet Resources

1. Mandatory application of ITU technical standards

- Another significant category of proposals deal with making the Recommendations that come out of ITU-T technical Study Groups mandatory for Member States
  - "Recommendations" are technical standards that allow for telecommunications infrastructure to interoperate: if equipment manufacturers all design their products using the same standards, then their equipment will be able to connect to and operate on the global telephony network.
  - Currently, ITU-T Recommendations are not binding, and cover a range of issues – including, for example, standardization of lawful intercept and deep packet inspection functionality.
- If Member States require that ITU standards that apply to Internet technology be made mandatory, this would represent a fundamental shift away from how Internet standards are currently being developed and could undermine the global interoperability of the Internet. The Internet works as a global network because it runs on a set of technical standards: these standards allow individuals connect to the Internet, access information, and communicate across borders online using technology and applications of their choice. Today, standards are largely developed through open, voluntary, consensus-based multistakeholder bodies such as the IETF and the W3C.[4] This method of standards development has been extremely successful and has remained flexible enough to respond to quickly evolving technological change.
- There is fear that a more top-down, mandatory process for standards development would undermine users' ability to connect to the Internet with technology of their choice, might undermine global interoperability, and would be too inflexible to keep up with the pace of change. Individuals and companies that may want to develop new kinds of online services and applications may face new barriers because they will have to do so within the standards set up by the ITU. The ITU's barriers to open participation only compound the impact.
- While individual states can make legal reservations to any part of the treaty, a reservation to this change would not protect users in a reserving state from being affected. Technological standards drive commercial development and design of technology – if enough member states adopt ITU Recommendations as mandatory, companies everywhere will not be willing to sell technology that doesn't comply with

[4] For a very brief overview of standards bodies, see http://www.publicknowledge.org/blog/internet-governance-way-it-works-now and http://www.internetsociety.org/what-we-do/standards.

those standards.
- In favor: Arab States (C 67), Egypt (C 81), Mexico, UAE, Iran (supporting various amendments that would make at least certain ITU-T recs mandatory)
- Against: UK, USA, CITEL (C 65), Netherlands, Portugal, Sweden, Korea, Bulgaria

2. IPv6 address allocation and Naming and Numbering Misuse
- Russia and Côte d'Ivoire support a proposal for the ITU to have some role in allocating some portion of IPv6 addresses.
- In addition, a few proposals have been put forward by Egypt, the Arab States, the African States regional groups, UAE, Cuba, and Iran to address misuse of naming, numbering, addressing, and identification resources (See section A.3. above). Depending on how these terms are defined, these proposals could have implications for Internet resources – for example, misuse of IP addressing or the domain name system.

D. Interconnection, Access, and Net Neutrality

1. ETNO proposal for charging, interconnect, and "quality of service"[5]
- The European Telecommunications Network Operators Association (ETNO) (an ITU Sector Member), has proposed a series of radical changes to the system of peering and interconnection between IP network providers – in short, how the various network of networks that make up the Internet connect so that information can flow seamlessly across the global Internet.
  - The proposal endorses a "sending party pays" approach to interconnection, where the "sender" of content may have to pay to reach the recipient. This approach comes from traditional international telephony, where the calling party's telephone network pays to complete a long distance call (and the receiving party pays nothing). In turn, the calling party's telephone network passes on the cost to the calling party.
  - The proposal would also require end-to-end "quality of service," which would encourage network operators to prioritize certain (unspecified) traffic to guarantee a certain level of performance. This concept undermines principles of net neutrality.
- While the proposal might benefit large, incumbent telecommunications operators, it will not likely expand Internet access in countries that need it most.
  - The proposal may lead to increased cost of Internet access for everyone. This result would impact most heavily those in less developed countries because content providers and companies may be less willing to pay to reach smaller markets. In turn, this limits users' rights to access information, ideas, and knowledge and raises the costs of offering their own content and services in the global online marketplace.
  - The proposal is also inconsistent with principles of net neutrality as it would encourage ISPs to prioritize certain traffic, content, or services, perhaps in the form of private agreements between ISPs and content providers.
- ETNO proposal (amending Art 2-4 in the ITRs): http://files.wcitleaks.org/public/ETNO%20C109.pdf

[5] For a full analysis of the implications of this proposal, see https://www.cdt.org/report/etno-proposal-threatens-access-open-global-internet and https://www.cdt.org/blogs/cynthia-wong/2106radical-proposal-now-table-itu.

2. International Internet Connectivity

- Paraguay remains committed to raising the profile of international connectivity challenges for landlocked and developing countries. It has not gotten support from other Member States within CITEL, in part due to concerns about including any Internet-specific issues in the ITRs. Paraguay's proposal could open the door to applying traditional public switched telephone network (PTSN) accounting rate settlements to Internet Protocol networks.

Key Acronyms	
Acronym	**Entity or Meeting**
Regional groups Upcoming meetings: http://www.itu.int/en/ITU-T/wtsa-12/prepmeet/Pages/default.aspx	
APT	Asia-Pacific Telecommunity http://www.apt.int/aptmembers
Arab States	Arab States regional group http://www.itu.int/ITU-D/arb/Aminstrations.html
ATU	African Telecommunication Union http://atu-uat.org/index.php/en/members
CEPT	European Conference of Postal and Telecommunications http://www.cept.org/cept/membership-and-observers
CITEL	Inter-American Telecommunication Commission of the Organization of American States http://web.oas.org/citel/en/Pages/default.aspx
RCC	Regional Commonwealth in the Field of Telecommunications http://www.en.rcc.org.ru/index.php/rcc/rcc-participants
Other terms	
CWG	Council Working Group – steering group of Member States for WCIT12. Membership: http://www.itu.int/council/groups/cwg-wcit12/
IETF	Internet Engineering Task Force – one of the primary standards development bodies for Internet technologies
IGF	Internet Governance Forum
ITR	International Telecommunication Regulations – the treaty being negotiated at WCIT12
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector – issues "Recommendations," which are standards for telecommunications
WCIT12	2012 World Conference on International Telecommunications
WSIS	World Summit on the Information Society
WTPF	World Telecommunication/Information and Communication Technology Policy Forum